

CVE-2009-0995: Oracle EBS - Unauthenticated Unchecked Redirect Vulnerability

Background

The Oracle E-Business Suite (EBS) is a collection of business Enterprise Resource Planning, Customer Relationship Management, and Supply Chain Management applications developed by Oracle Corporation. Interaction with the client is achieved through the Apache web server, Java technology (Applets) and several other Oracle technologies. Business data is stored in the Oracle database.

Scope

Imperva's Application Defense Center is conducting a research of various business applications in order to devise better security solutions for them. The team generates reports of this sort when web application vulnerabilities are identified as part of the research.

Findings

An unchecked redirect vulnerability was discovered. This vulnerability can be exploited for stealing sensitive data and executing Phishing attacks. More specifically, data can be stolen from the users of the business suite, whether these are employees of the organization that deploys EBS or partners that access it in a self-service mode. In addition, arbitrary code can be sent to a user while the address bar of the browser shows the EBS server's URL. For example, a spam email that claims to link to an automatic patch installation URL can compromise user's systems.

Exploit

```
http://first.imperva:8003/OA_HTML/OA.jsp?_rc=FNDPORTALRELEASEAM&_ri=0&retainAM=N&_userOrSSWAPortalUrl=http%3A//www.imperva.com&_ti=587762657&oapc=2&oas=RmquZ-H2Bh9OH2LSz-o_Rg..
```

Tested Versions

Vulnerable

Oracle applications release 11i

Vendor Status

14-Jun-07 Vendor notified

Fixed in April 2009 CPU

Discovered By

Guy Karlebach